Steps:

1. Answer Forensics Questions
2. Windows Updates (Restart Later)
3. Users – Add/Remove
4. User Account Types – Confirm users have correct account type
5. Audit existing users to confirm they are set up correctly
6. Passwords – Make sure current users passwords are appropriate.
7. Firewall - Make sure it is on
8. Microsoft Security Baseline Assessment
9. Readme Info – Follow readme directions
10. Add/Remove Software – Confirm only allowed software is on the computer
11. Software Updates (ex. Firefox, libra, adobe, etc.)
12. Set Password policies - Make sure you have strong password policies
13. Group Policies –
14. Audits – Turn on auditing
15. Services: Enable/disable – Make sure appropriate services are running
16. Check ports – Make sure nothing is open that shouldn’t be
17. Antivirus (download, Update, Run scan)
18. Browser Security Settings – don’t auto download, etc.
19. Internet Options
20. Easter Egg Hunt (File Searching, Turn on Hidden Files, look for forbidden file types)
21. Check scheduled tasks - make sure the attacker has not set a scheduled task called something else to start back up after you remove the threat.
22. Look at process for anything unusual - https://www.processlibrary.com/en/
23. Turn on bit locker
24. Resources/ Task Manager/ Start-up – See if anything is taking up too many resources
25. Use Windows Admin tools in Control Panel
26. Restart For Windows Updates